BURNS

The Foundation Period in the History of Group Theory

Mathematics

A. M.

1911

THE FOUNDATION PERIOD IN THE HISTORY OF GROUP THEORY

BY

JOSEPHINE ELIZABETH BURNS
A. B. University of Illinois, 1909

THESIS

Submitted in Partial Fulfillment of the Requirements for the

Degree of

MASTER OF ARTS

IN MATHEMATICS

IN

THE GRADUATE SCHOOL

OF THE

UNIVERSITY OF ILLINOIS

1911

UNIVERSITY OF ILLINOIS

THE GRADUATE SCHOOL

June 2 1911

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

JOSEPHINE ELIZABETH BURNS

ENTITLED The Foundation Period in the History of Group Theory

BE ACCEPTED AS FULFILLING THIS PART OF THE REQUIREMENTS FOR THE

DEGREE OF Master of Arts

G. A. Miller
In Charge of Major Work

E. J. Townsend
Head of Department

Recommendation concurred in:

Committee
on
Final Examination

TABLE OF CONTENTS.

Henri Poincaré has pointed out that the fundamental conception of a group is evident in Euclid's work; in fact that the foundation of Euclid's demonstrations is the group idea.(1) Poincare establishes this assertion by showing that such operations as successive superposition and rotation about a fixed axis presuppose the displacements of a group. He shows that the axioms of Euclid which are easily referred to the group concept are those omitted in Euclids work, and that those axioms which may be referred to the group concept with more difficulty, are the axioms explicitly enunciated. However much the fundamental group notions are dormant in the work of early mathematicians, it was not until the latter part of the eighteenth century that these notions began to take life and develop. The period of foundation of group theory as a distinct science extends from Lagrange (1770) to Cauchy (1844-6) a period of about seventy five years. We find Lagrange considering the number of values a rational function can assume when the variables are permuted in every possible way. With this beginning the development may be traced down through the contributions of Vandermonde, Ruffini, Abbati, Abel, Galois, Bertrand, and Hermite to Cauchy's period of active production (1844-1846). Group theory was at the beginning of the period a discovery useful in the consideration of the theory of equations; at the end it existed as a distinct science, not yet, to be sure, entirely freed from the restrictions of applications to other branches but sufficiently so that this may be considered the close of the foundation period. In the first part of this paper we shall consider briefly the contributions of the more important men from Lagrange

---

(1) The Monist 9, 1898, pp. 1-43.

to Cauchy, and in the second we shall attempt a more critical study of the contributions of Cauchy; for his work may be considered the culmination of this formative period.

Lagrange.

The contributions of Lagrange are included in his memoir "Reflexions sur la résolution algébrique des equations" published in the Mémoires of the Academy of Science at Berlin in 1770-1771.(1) In this paper Lagrange first applies what he calls the "calcul des combinaisons" to the solution of algebraic equations. This is practically the theory of substitutions, and he uses it to show wherein the efforts of his predecessors, Cardan, Ferrari, Descartes, Tschirnhaus, Euler and Bézout fail in the case of equations of degree higher than the fourth. He studies the number of values that a function can assume when the variables are permuted in every possible way. The theorem that the order of a subgroup divides the order of the group is implied but not explicitly proved. The theorem that the order of a group of degree n divides n! is however explicitly stated. (3) Lagrange does not use at all the notation or terminology of group theory but confines himself entirely to the direct applications to the theory of equations. His symmetric group of order 24,(2), if such it may be called, he writes in the following form:

$f\left[(x^{i})\,(x^{ii})\,(x^{iii})\,(x^{iv})\right]$

$f\left[(x^{iii})\,(x^{ii})\,(x^{i})\,(x^{iv})\right]$

$f\left[(x^{i})\,(x^{iii})\,(x^{ii})\,(x^{iv})\right]$

$f\left[(x^{iv})\,(x^{ii})\,(x^{iii})\,(x^{i})\right]$

$f\left[(x^{iii})\,(x^{ii})\,(x^{iv})\,(x^{i})\right]$

$f\left[(x^{iv})\,(x^{iii})\,(x^{ii})\,(x^{i})\right]$

$f\left[(x^{i})\,(x^{iV})\,(x^{iii})\,(x^{ii})\right]$

$f\left[(x^{ii})\,(x^{i})\,(x^{iii})\,(x^{iv})\right]$

$f\left[(x^{ii})\,(x^{iii})\,(x^{i})\,(x^{iv})\right]$

$f\left[(x^{iii})\,(x^{i})\,(x^{ii})\,(x^{iv})\right]$

$f\left[(x^{ii})\,(x^{iv})\,(x^{iii})\,(x^{i})\right]$

$f\left[(x^{ii})\,(x^{iii})\,(x^{iv})\,(x^{i})\right]$

$f\left[(x^{iii})\,(x^{iv})\,(x^{ii})\,(x^{i})\right]$

$f\left[(x^{iv})\,(x^{i})\,(x^{iii})\,(x^{ii})\right]$

---

(1) Oeuvres de Lagrange, Vol. 3, pp. 204-420
(2) Ibid, p. 394
(3) Ibid, p. 372

$f\left[(x^{iii})\,(x^{iv})\,(x^{i})\,(x^{ii})\right]$ $f\left[(x^{iv})\,(x^{iii})\,(x^{i})\,(x^{ii})\right]$
$f\left[(x^{i})\,(x^{iii})\,(x^{iv})\,(x^{ii})\right]$ $f\left[(x^{iii})\,(x^{i})\,(x^{iv})\,(x^{ii})\right]$
$f\left[(x^{i})\,(x^{ii})\,(x^{iv})\,(x^{iii})\right]$ $f\left[(x^{ii})\,(x^{i})\,(x^{iv})\,(x^{iii})\right]$
$f\left[(x^{iv})\,(x^{ii})\,(x^{i})\,(x^{iii})\right]$ $f\left[(x^{ii})\,(x^{iv})\,(x^{i})\,(x^{iii})\right]$
$f\left[(x^{i})\,(x^{iv})\,(x^{ii})\,(x^{iii})\right]$ $f\left[(x^{iv})\,(x^{i})\,(x^{ii})\,(x^{iii})\right]$

The four group and the cyclic group of order four are both given as subgroups of this symmetric group.

This is practically all that can be said of the contributions of Lagrange to the theory of substitution groups. He was on the right path but he hardly went far enough to gain for himself the credit for the establishment of the theory of substitutions.

Ruffini.

What was begun by Lagrange was carried on and amplified by his disciples. The first man who followed him and made any signal additions was Paolo Ruffini, an Italian, who published in 1799 in his Teoria generale delle equazioni, a number of theorems important in the theory of substitutions. According to Burkhardt(1), several fundamental concepts are implied here, if not explicitly stated. Ruffini's "Permutation" corresponds to the later accepted term of group and Cauchy's "System of Conjugate Substitutions". These "permutations" he classifies first into "simple" and "complex". The first are of two sorts, of one cycle or of more than one cycle. The second are divided into three classes which correspond to the modern notions (1) of intransitive, (2) of transitive imprimitive, and (3) transitive primitive. Burkhardt says that Ruffini paved the way

(1) Der Anfange der Gruppentheorie und Paolo Ruffini Zeitschrift fue Mathematik und Physik (1892) 37, p. 119.

for the concept of the invariant subgroup which was first used by Galois. Ruffini used the term degree for the order of his "permutation" or "grado di uguaglianza".

Ruffini confined himself to the group theory that arose in connection with the theory of equations, and we do not yet see any indications of a break between the two. He studied the number of values a function can assume when the variables are permuted in every possible way. Some of his theorems are:

(1) If a substitution of n letters leaves the value of a rational function invariant, the result of applying this substitution any number of times is that the function is left invariant.

(2) The order of a substitution is the least common multiple of the orders of the cycles.

(3) The order of a subgroup divides the order of the group.

This theorem, here stated again, was not completely proved till 1802 when Abbati satisfactorily established it.

(4) There is not necessarily a subgroup corresponding to every arbitrary divisor of the order of a group.

This he established by showing that there is no eight, three or four valued function on five letters.

(5) A primitive group of degree five that contains no cycle of degree five can not have its order divisible by five.

These theorems are the most important of those established by Ruffini, and with the exception of the contributions of Abbati, constitute the most important work that was done down to the time of Galois. To Abbati group theory owes the complete proof that the order of the subgroup divides the order of the group. This he proved by putting the substitutions of the group in rectangular array. To

Abbati is also due the proof that there is no three or four valued function on n letters when n is greater than five. While Cauchy published one memoir during the long period of silence from Ruffini to Galois, it was of less importance than his significant contributions of 1844-1846, and we may leave its discussion until his work as a whole is considered. While the work of Abel added practically nothing to the theory of substitutions, still his name should not be omitted from the list of founders for by his use of substitution theory to prove that it is impossible to solve algebraically equations of degree higher than the fourth, he called attention to the instrument he used. This brings us to the work of Galois, written in 1831 and 1832, but not made public until 1846.

Galois.

Up to the time of Cauchy, Galois was undoubtedly the man who accomplished the most along the line of substitution theory. To Galois is due the credit for broadening and strengthening the connection between the theory of equations and the theory of substitutions. Galois developed a number of fundamental notions in group theory, but these were so inseparably connected with his theory of equations that he can scarcely be considered the founder of the science. His work is also important in the same sense in which Abel's is. His use of substitution theory tended to call attention to the subject.

To Galois, first of all, credit is due for the conception of the invariant subgroup, (1) and had his contributions been nothing other than this, his place as a pioneer in group theory would be per-

---

(1) Galois: Oeuvres, p. 26.

manently established. Although this powerful utensil in the study of groups was neglected largely by his immediate successors, notably by Cauchy, it is none the less important to note its presence here.

Other notions due to Galois are that of simple group and the extension of the idea of primitivity. Galois first used the term group in its present technical sense.

His definition of the group of an equation is as follows:

"Given an equation with roots a, b, c - - -. There will be a group of permutations that have the properties:

(1) that all functions of the roots that are left invariant by the substitutions of this group are rationally known; and

(2) that every function of the roots rationally determined is left invariant by the group of substitutions."

Other theorems stated without proof by Galois :

The lowest possible composite order of a simple group is 60 (1).

The substitutions common to two groups form a group (2).

If the order of a group is divisible by p, a prime, the group contains a substitution of order p (2).

The substitutions of a group that omit a given letter form a group (2).

For subgroup Galois says "divisor" (3) for simple group, an indecomposable group (4). These include the more important things to be mentioned in connection with Galois's work. Although to a large extent only the results are stated, still these results

(1) Oeuvres Mathématiques d' Évariste Galois, p. 26
(2) Manuscrits de Évariste Galois, p. 39
(3) Oeuvres, p. 58
(4) " , p. 26.

are of fundamental importance, and had he succeeded in making the break between substitution theory and the theory of equations more pronounced, his work instead of Cauchy's might now be considered the corner stone of group theory.

Cauchy.

In the present section our purpose is two-fold. In the first place, by indicating the main theorems and proofs presented by Cauchy in his Exercises d' analyse et de physique mathématique (1844) and in the series of articles published in the Paris Comptes rendus des séances de l' académie des sciences (1845-46) (1), we shall attempt to show to what an extent Cauchy deserves the credit for establishing the theory of groups as a distinct science. The second purpose is to call attention to such errors occurring in the above mentioned articles as have not yet been noted. Before carrying out these two purposes, however, it might be well to consider rather briefly the notation and terminology used by Cauchy, especially where these differ from the notation and terms used by subsequent writers on the subject and where the terms originated by Cauchy have won a permanent place in modern group theory language.

In his earliest article on the subject of substitutions, Cauchy uses the word substitution in the sense it now possesses and defines it in that sense; (2) but in the first of his articles published in the Paris Comptes rendus, he defines permutation and substitution in the same way, as he does also in the Exercises (3) (4).

---

(1) Oeuvres de A. Cauchy, 1st serie IX, X
(2) Journal de l' École Polytechnique 10, 1815, p. 3
(3) Oeuvres de A. Cauchy, 1st serie IX, p. 280
(4) Exercises d' analyse et de physique mathematique III, p. 152

Throughout his work however he uses the term substitution more commonly. His notation, as he first denotes a substitution, is awkward but after defining this notation, he leaves it for a simpler and does not again return to it. The notation $\begin{pmatrix} x & z & y \\ x & y & z \end{pmatrix}$ means that x is replaced by itself by the substitution, that y is replaced by z, z by y, the lower letter by the one above. He also uses the notation $\left(\frac{y\ z\ --\ v\ w\ x}{x\ y\ --\ u\ v\ w}\right)$, where each letter below is replaced by the one above it. But the much more commonly used notation is (x, y, z, u, v), where each letter is replaced by the one which follows it and the last by the first. He defines this as a cyclic substitution(1). In the article written in 1815 (2) he defines the "degree" of a substitution as the first power of the substitution that reduces to identity, but later he also defines order in this way (3) and uses the word order rather than degree in his subsequent work. He uses both of the terms "unity" and "identical substitution"(4). A transposition (5) is defined and the terms similar (6), regular (7), inverse (6) and permutable substitutions (8) are found with their present significance. If we pass on from substitutions to groups, we find a group is a "system of conjugate substitutions", which may be transitive or intransitive (9). A transitive imprimitive group is "transitive complex"(10). The order of a system of conjugate substitutions is the number of substitutions it contains. The term

(1) J.Ec. polyt. 10, 1815, p. 13
(2) Oeuvres IX, p. 285
(3) Oeuvres IX, p. 283
(4) J.Ec.polyt. 10, 1815, p. 13
(5) Ibid, p. 18
(6) Exercises, v. III, p. 165
(7) Ibid, p. 162
(8) Oeuvres IX, p. 283, p. 290
(9) Ibid, p. 294
(10) Ibid, p. 311

"diviseur indicatif" is also found for the order of a group. Cauchy frequently transfers his definition of order to the theory of equations and speaks of the number of equal values a function can assume when the variables are permuted in every possible way. The number of distinct values of the function is the index (1). A final word may be said about the order of operation. In the Journal de l' Ecole polytechnique (10 p. 10) we find

$\begin{pmatrix} A_1 \\ A_6 \end{pmatrix} = \begin{pmatrix} A_2 \\ A_3 \end{pmatrix}\begin{pmatrix} A_4 \\ A_5 \end{pmatrix}$ indicates that $\begin{pmatrix} A_1 \\ A_6 \end{pmatrix}$ is the result of applying first the substitution $\begin{pmatrix} A_2 \\ A_3 \end{pmatrix}$, then the substitution $\begin{pmatrix} A_4 \\ A_5 \end{pmatrix}$; but in all the later work we find that the order of operation is reversed and the substitution $P\ M\ P^{-1}$ indicates operation from right to left. As a whole Cauchy's notation is clear; but there are many places where his meaning becomes very obscure due to piling up, all in the same discussion, several different alphabets with an abundance of subscripts and superscripts both needless and confusing.

We turn now to speak of the theorem proved and the concepts originated by Cauchy upon which are based his claims as the founder of group theory. In order to judge better just what advances he made, it might be well to state briefly what he had to build on, what were the specific things included in the work of his predecessors which he could use. Among these are the following:

(1) The order of a subgroup divides the order of the group.

(2) The concepts, not the terms, of primitivity and transitivity.

(3) The notion of an invariant subgroup.

(4) The theorem, not the proof, that if the order of the

---

(1) J. Ec. polyt. 10, (1815), p. 6

group is divisible by P, a prime, there is at least one substitution of order p.

These theorems and concepts are the ones which might have been of great help to Cauchy. We find that he uses the work of the earlier writers, but that he seems almost in ignorance of what Galois has done. In no place is explicit use made by Cauchy of the invariant subgroup. We might almost say implicit use too, for only in a few places does he seem to be getting close to this subject and then he seems to ignore entirely the immediate consequence of an invariant subgroup, the quotient group. So it is safe to conclude that Cauchy was almost absolutely uninfluenced by the work of Galois.

While Cauchy's important work did not appear until 1844-6, his article in the Journal de l' Ecole polytechnique, in 1815, contains some things that might well be mentioned. In this paper Cauchy first defines his terms and notation, then shows briefly the theorem already proved by Lagrange and Abbati, that the number of equal values of a function, the "diviseur indicatif" as he calls it, must divide n!. Then, after showing that it is always possible to construct a one or two valued function on n variables, he enunciates the theorem. The number of distinct values of a non symmetric function can not be less than the largest prime that divides n, without becoming equal to two. This theorem he then proves. This constitutes the most important theorem in this early paper although there are other things of interest.

If the degree of a function is a prime (1) number, the number of distinct values can not be less than the degree. If the de-

---

(1) Journal de l' Ecole Polytechnique, 1815, p. 19

gree is six, the number of distinct values can not be less than six when more than 2 (1). He definitely mentions the functions corresponding to (1) the intransitive group of degree 6 and order 36; (2) the intransitive group of degree 6 and order 48; (3) the transitive imprimitive group of degree 6 and order 72; and the symmetric group of degree 5, considered as an intransitive group of degree 6. The functions he gives are as follows:(2)

(1) $a_1 \quad a_2 \quad a_3 + 2a_4 \quad a_5 \quad a_6$

(2) $a_1 \quad a_2 \quad a_3 \quad a_4 + a_5 \quad a_6$

(3) $a_1 \quad a_2 \quad a_3 + a_4 \quad a_5 \quad a_6$

(4) $a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 + a_6$

He then shows that a function on six letters can not have more than six distinct values. This practically concludes the important things in Cauchy's early paper. One slight error is all that has been noted in this early article. Attention will be called to it later.

Cauchy's Memoir published in 1844 in his Exercises d'Analyse et de Physique Mathématique contains much more of value than did the earlier article. The first of this memoir is taken up principally with definitions which have been largely reproduced in the paragraph on notation and terminology. The first theorem proved is, that every substitution similar to a given substitution, P, is the product of three factors, the extremes of which are the inverse of each other and the middle term of which is P. Conversely, every product of three factors, the first and last of which are the inverse of each other, is similar to the middle term P. (3).

---

(1) Journal de l' Ecole Polytechnique, 1815, p. 20
(2) " " " " " , " , p. 23
(3) Exercises, Vol. 3, p. 169

An important formula developed is for the number of substitutions similar to a given substitution. This is the total number of substitutions possible on n letters divided by the number of substitutions that transform the given substitution into itself(1). Cauchy states the formula and proves it. If $\bar{w}$ is the number required, n the number of letters and P the given substitution, composed of f cycles of order a, g cycles of order b, h cycles of order c, - - etc. - -, and r the number of letters fixed in P, then

$$\bar{w} = \frac{n!}{(f!)\,(g!)\,(h!)\,-\,-\,(r\,)!\,a^{f}\,b^{g}\,c^{h}} \quad (2)$$

Then $\sum \bar{w} = n!$ and

$$\sum \frac{1}{(f!)\,(g!)\,(h!)\,(r!)\,a^{f}\,b^{g}\,c^{h}} = 1$$

This last formula he leaves thus in the Exercises, but he returns to it in a later memoir among those published in the Paris Comptes rendus and uses it in the development of some important formulas in which is implied the theorem that the average number of letters in the substitutions of a transitive group of degree n is n - 1.

A number of important theorems relative to substitutions are developed, which may be quoted as follows:

(1) The order of a substitution is equal to the least common multiple of the order of the cycles that compose it(3). This theorem has been already referred to Ruffini.

(2) If P is a substitution of order i, h any number, and θ the highest common factor of h and i, then P^{h} will be of order $\frac{i}{\theta}$ (4).

(1) Exercises, Vol. 3, p. 169
(2) " , Vol. 3, p. 173
(3) " , " ", p. 202
(4) " , " ", p. 203

(3) If P is a substitution of order i, the substitutions among the powers of P that are of order i, are the powers of P whose indices are prime to i. These substitutions are likewise similar to P and so the number of substitutions similar to P among its powers are in number equal to the number of numbers prime to i and less than i (1).

(4) Let P be any substitution, regular or irregular; let i be its order, and p a prime factor of i. Then a value for l can always be found such that P^l is a substitution of order p (2).

(5) A substitution and its inverse are always similar (3).

(6) The powers of a cycle constitute the totality of substitutions that transform the given cycle into itself (4).

(7) If Q, R, S, - - are different substitutions that are permutable with P, then the product of two or more in any order is permutable with P (5).

(8) The inverse of $P^h Q^k$ is $Q^{-k} P^{-h}$ (6).

After defining a group, calling it a system of conjugate substitutions, Cauchy states and proves a number of important theorems.

(1) The order of a system of conjugate substitutions always divides n!(7).

While of course this theorem is not due to Cauchy, still his statement of the proof is simple and clear.

(1) Exercises, Vol. 3, p. 203
(2) Ibid, Vol. 3, p. 209
(3) Ibid, Vol. 3, p. 209
(4) Ibid, " ", p. 221
(5) Ibid, " ", p. 224
(6) Oeuvres, Vol. 9, p. 325
(7) Exercises, Vol. 3, p. 184

(2) (1) The order of a system of conjugate substitutions is divisible by the order of each substitution.

(3) (2) This theorem may be enunciated in group theory language as follows:

Two permutable substitutions with no common power but identity, together generate a group whose order is the product of the orders of the substitution.

* The theorem is then extended to any number of substitutions fulfilling the same conditions. A special case is developed where the substitutions are all on different letters and so give rise to an intransitive group.

There is developed here a unique way of building a cyclic group (3). The general method he develops may be applied to a specific case as follows:

Given a regular substitution P, say of degree 12, with 3 cycles of order 4.

P = abcd · efgh · ijkl. If then these three cycles be written in three horizontal rows

abcd

efgh

ijkl

the substitution Q, formed by taking each vertical row as a cycle,

---

* In the future we shall confine ourselves to group theory language except in so far as a clear statement of Cauchy's thought requires us to follow his terminology also.

(1) Exercises Vol. 3, p. 185

(2) Ibid, p. 189

(3) Ibid, p. 191

Q = aei·bfj·cgk·dhl, will be permutable with P and P and Q will generate the cyclic group of order 12. The products may be arranged as follows:

$$\begin{array}{llll} Q & P & P^2 & P^3 \\ Q & PQ & P^2Q & P^3Q \\ Q^2 & PQ^2 & P^2Q^2 & P^3Q^2 \end{array} \qquad \text{or} \qquad \begin{array}{llll} Q & P & P^2 & P^3 \\ Q & QP & QP^2 & QP^3 \\ Q^2 & Q^2P & Q^2P^2 & Q^2P^3 \end{array}$$

The substitutions then are:

1 : abcd·efgh·ijkl : ac·bd·eg·fh·ik·jl : adcb·ehgf·ilkj
aei·bfj·cgk·dhl : afkdej chebgl : agriek·bhjdfl : ahkbel cfidgj
aie·bjf·ckg·dlh : ajgdif clebkh : akecig · blfdjh : algbih cjedkf

(4) If $1\ P_1\ P2\ P_3 - - - P_{a-1}$
$1\ Q_1\ Q_2\ Q_3 - - - Q_{b-1}$ are two groups, one of order a, the other of order b, that are permutable, and have no common terms other than the identity, then the group generated by these two groups is of order ab (1).

(5) If two groups $1\ P_1\ P_2\ P_3 - - - P_{a-1}$
$1\ Q_1\ Q_2\ Q_3 - - - Q_{b-1}$ one of order a and the other of order b, generate a third group of order ab, then the two groups are permutable (2).

The illustrative example which Cauchy gives is the group that belongs to the function

$$\Omega = (x - y)(x - z)(y - z)(y - u)(z - u).$$

$P_1 = xy·zu$ $P_2 = xz·yu$ $P_3 = xu·yz$

gives the four group.

$Q = yzu$ $Q^2 = yuz$ gives the cyclic group of order three. The product of the two groups is the alternating group of degree four and order twelve.

---

(1) Exercises, Vol. 3, p. 229
(2) Ibid, p. 229.

(6) If P and Q are two substitutions, one of order a and the other of order b, and if the two series

$$Q \quad PQ \quad P^2 \quad - - - - \quad P^{a-1}Q$$

$$Q \quad QP \quad QP^2 \quad - - - - \quad QP^{a-1}$$

are made up of the same terms, in the same or different orders, then the cyclic group generated by P is permutable with the cyclic group generated by Q(1).

(7) If $1 \quad P_1 \quad P_2 \quad - - - \quad P_{a-1}$

$1 \quad Q_1 \quad Q_2 \quad - - - \quad Q_{b-1}$ are two groups, of orders a and b respectively, if $n!$ is not divisible by ab then at least one P_α is similar to a Q_β (2).

One of the most important theorems, if not the most so, proved by Cauchy in the Exercises is that one usually called Cauchy's theorem.

If M is the order of a group and p any prime that divides M, then the group contains at least one substitution of order p (3).

Since this theorem is so fundamental, especially as it is a big step towards Sylow's theorem which appeared nearly thirty years later, it may be considered as a most important element in the establishment of Cauchy's claim as the founder of group theory.

Besides the theorems proved in the Exercises, there are a number of specific groups mentioned. No enumeration of groups of special degrees is attempted, but in several cases the substitutions are written out. Those given are :

(1) The octic as an example of a group generated by the substitutions permutable with a given substitution (4).

(2) Intransitive group of degree six and order 9, the

---

(1) Exercises, Vol. 3, p. 229
(2) Exercises, p. 249, Vol. 3
(3) " , p. 250, Vol. 3 Enunciated but not proved by Galois, but proved by Cauchy. Manuscrits de Evariste Galois, p. 39.
(4) Ibid, p. 198

direct product of two cyclic groups of order 3 (1).

(3) The intransitive group of order 16 and degree 6, with the two systems of intransitives, four and two (2).

(4) The holomorph of the cyclic group of order 5 (3).

(5) The four group (4).

In addition to these groups whose substitutions are given, other specific groups mentioned are:

(1) the holomorph of order 42 (5)

(2) the group of degree 7 order 21 (6)

(3) the holomorph of the cyclic group of order 9 (6).

There is also mentioned (6) a group of degree 9, of order 27, generated by the two substitutions

$$P = x_0\,x_3\,x_6 \cdot x_1\,x_4\,x_7 \cdot x_2\,x_5\,x_8$$

$$Q = x_1\,x_2\,x_4\,x_8\,x_5 \cdot x_3\,x_6$$

Obviously this is impossible, but a little study of his method reveals that the Q should be $Q = x_1\,x_2\,x_4\,x_8\,x_7\,x_5 \cdot x_3\,x_6$ and that in order to get the order of the group he has made a misapplication of the theorems he has just enunciated and which he is illustrating; that the order of the group should be 18. The two theorems he is illustrating may be stated as follows:

(1) (7) If P is a substitution on n letters as $P = x_0\,x_1\,x_2 - - - x_{n-1}$, and if r is any number prime to n, and Q is a substitution derived from P by replacing each letter by another whose sub-

---

(1) Exercises, Vol. 3, p. 199
(2) Ibid, p. 200
(3) Ibid, p. 244
(4) Ibid, p. 239
(5) Ibid, p. 240
(6) Ibid, p. 235
(7) Ibid, p. 239

script is r times its own, then for any values of h and k

$$Q^k P^h = P^{r^k h} Q^k .$$

(2) (1) If in the above theorem we take τ any divisor of n distinct from unity and let R be the substitution that replaces any letter x by the letter with the exponent $x_{\ell+r}$, then $Q^k P^h$ generate a group of order τi where i is the smallest value of k that satisfies $r^k = 1 \mod n$.

Since r is 2 in the case at hand then i must be 6. The order of the group then is $\tau i = 3 \cdot 6 = 18$ whereas Cauchy seems to take $i = 9$, and so derives the order of the group $3 \cdot 9 = 27$.

We turn now to Cauchy's Memoirs published in the Paris Comptes rendus (1845-6). Some of the material in these memoirs had already appeared in the Exercises but is more extensively treated in the Memoirs. Much that is given, too, in the latter is not touched upon in the former. We shall omit here such things as have already been mentioned in the paragraph on the Exercises except in so far as their extension in the later Memoirs make a repetition profitable.

After fundamental definitions of the terms used, we find a group defined as follows:

" I shall call derived substitutions all those that can arise from the given substitutions by multiplying them one or more times by each other or by themselves, and the given substitutions together with all the derived substitutions form what I shall call a system of conjugate substitutions." (2).

Then follow the general theorems:

(1) If i is the order of a substitution P and a, b, c, - -

---

(1) Exercises, p. 235, Vol. 3
(2) Cauchy Oeuvres, Vol. 9, Ser. 1, p. 290

are the prime factors of i, then the substitution P and its powers form a group generated by the substitutions

$$P^{\frac{i}{a}},\ P^{\frac{i}{b}},\ P^{\frac{i}{c}}\ -\ -\ -\ .$$ (1)

(2) (2) If P, Q, R, S - - - are the substitutions that leave a given function Ω invariant, they form a group whose order is the number of equal values of Ω .

(3) The order of a transitive group of degree n is n times the order of the subgroup that leaves one letter fixed. (3)

(4) If Ω is a transitive function on n letter, if m is the index of the corresponding transitive group under the symmetric group of degree n, then m will likewise be the index of the subgroup that leaves one letter fixed under the symmetric group of degree n - 1. (3)

The general subject Cauchy treats next is that of intransitive groups (4). He implicitly divides intransitive groups into two sorts. The first are those where the systems are independent as he says, in our terminology, where the systems are united by the direct product.

The second sort are those where the systems are dependent, or as we say, are united by some sort of an isomorphism. The concept of isomorphism is however only implied. He states first that an intransitive group is formed by the combination, in some way, of transitive constituents. He then develops some interesting formulas for the orders of intransitive groups. If the systems are "independent" then M, the order of the group, is the direct product of

---

(1) Oeuvres, Vol. 9, p. 292
(2) " , Vol. 9, p. 336
(3) " , " ", p. 295
(4) " , " ", p. 296-303

A, B, C - - -, the orders of the transitive constituents and the index will be $\frac{n!}{A,\ B,\ C - - -}$ where a, b, c - - are the degrees of the constituents. (1)

This same formula holds also when the systems are not independent if A, B, C - - - are defined in a special way. They may be defined as follows:

Let A be the order of the first transitive constituent;

Let B be the number of substitutions involving letters of the second system without involving any of the first;

Let C be the number of substitutions involving letters of the third system without involving any of the first or second.

With these definitions then the order of the intransitive group is $M = A\ B\ C - - - -$. By putting $A' = \frac{a!}{A}$ $B' = \frac{b!}{B}$ $C' = \frac{c!}{C}$ - - - and $N' = \frac{n!}{a!\,b!\,c!}$, then m, the index of the intransitive group under the symmetric group is given by the formula $m = N'\ A'\ B''\ C' - - -$, where N' is the coefficient of the product $r^a\ s^b\ t^c - - -$ in the expansion of the polynomial $(r + s + t - - -)^n$.

After considering intransitive groups Cauchy turns to imprimitive groups. Here he confines himself almost entirely to the consideration of those imprimitive groups which are simply transitive and which have for the subgroup that leaves one letter fixed the direct product of the transitive constituents. In regard to this particular type of imprimitive groups, he gives several theorems which are of interest even though he does not touch upon the broader and more general principles.

If we have a simply transitive group such that the sub-

(1) Oeuvres, Vol. 9, p. 298

group that leaves one letter fixed is an intransitive group formed by the direct product of its transitive constituents, then the group is imprimitive. He considers the special cases when a, the number of letters in the largest transitive constituent, is greater than $\frac{n}{2}$, when n is the degree of the group, where a is less than $\frac{n}{2}$ and when a is equal to $\frac{n}{2}$, and in the second case illustrates his theorem by a special example.

The only theorems which he enunciates that apply to imprimitive groups in general are, (1) that the number of letters in the systems of imprimitivity must be a divisor of the degree, and (2) that if A is the number of substitutions that permute the variables within the systems and K the number of ways the k systems can be permuted then the order of the group will be $K A^k$.

An erroneous theorem in regard to imprimitive groups to which attention has already been called, is as follows:

"If G_1 is the subgroup which is composed of all the substitutions which omit a given letter of a simply transitive group G_1 then G is imprimitive unless all of the transitive constituents of G_1 are of the same degree". (1)

There is an interesting theorem with regard to symmetric groups which is worth quoting.

"If a transitive group of degree n has a symmetric subgroup of degree a, where $a > \frac{n}{2}$, then the group is symmetric on n letters.

---

(1) Oeuvres de Cauchy, Vol. 9, p. 443.
The error is noted in "Historical sketch of the development of the theory of groups of finite order" by G. A. Miller. Bibliotheca Mathematica (1910), Ser. 3, Vol. 10, p. 321.

The corollaries added are:

(1) $n > 2$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of order $n - 1$.

(2) $n > 3$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 2$. The special case $n - 4$ is excepted here for the octic group belonging to the function $\Omega = xy + zu$ is symmetric on two letters, yet is not symmetric on all four.

(3) $n > 4$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 3$. The case where $n = 6$ is excluded here. A group requiring that this exception be made is the imprimitive group of degree 6 and order 72 which contains the symmetric group of order 6.

(4) $n > 5$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 4$. If $n = 6$ or $n = 8$, this does not hold. Cauchy gives as examples of the case when $n = 6$, the imprimitive groups of degree 6, of orders 72 and 48.

One of the most interesting parts of Cauchy's work on group theory is that in which he develops the formulas from which can be deduced the theorem that the average number of letters in the substitutions of a transitive group is $n - 1$. In general his method may be summed up thus:(1)

Consider a transitive group of degree n, that is intransitive when ℓ letters become fixed, that is, it is ℓ-fold transitive. Consider the number of substitutions in this group which are similar to a given substitution P; then the number of substitutions similar to P in the subgroup that leaves ℓ letters fixed. As P assumes all

---

(1) Oeuvres, Vol. 9, pp. 384-395

possible forms, then the sum of all the substitutions similar to P gives the order of the group. The number of substitutions similar to P in the whole group is found in terms of ℓ and the number of omitted letters in P. Summing these numbers as the form of P is allowed to vary, gives various expressions for the order of the group and from these the theorems are deducible.

With this brief outline of the general method we can now go more into detail.. For convenience in reference we shall for the most part keep Cauchy's notation.

Given a group G of degree n and P a substitution in this group of order i.

Let $\bar{w}$ be the number of substitutions similar to P possible on n letters.

Let h be the number of such substitutions included in the group.

Let k be the number of conjugates of G under the symmetric group, that contain P.

Let M be the order of the group and m its index under the symmetric group of degree n.

Then $\frac{h}{\bar{w}} = \frac{k}{m} = 1$, for $hm = k\bar{w}$, since h is the number of substitutions similar to P in the group which is a subgroup of the symmetric group. There are m conjugate subgroups of this sort so in these m subgroups the number of substitutions, involving repetitions, similar to P is hm . There are $\bar{w}$ substitutions possible similar to P in the symmetric group and each is repeated k times. So for the total number of substitutions appearing in the m conjugate subgroups of the symmetric group involving repetitions we have $k\bar{w}$. But the two must be the same so

$$hm = k\bar{w}$$

It is easily seen that the ratio $\frac{h}{\bar{w}} = \frac{k}{m}$ can not exceed one since the total number of substitutions similar to a given substitution in any group can not exceed the total number of such substitutions in the symmetric group involving this group as a subgroup.

$\sum h = M$ when the sum is taken over all the values of h corresponding to different forms of P.

Consider G ℓ-fold transitive.

Let h' be the number of substitutions similar to P in the subgroup that leaves ℓ letters fixed, $\bar{w}$ the number of substitutions that can be formed similar to P, on n - 1 letters, and M' the order of the subgroup that leaves ℓ letters fixed.

Then $hm = k\bar{w}$ becomes for this subgroup $h'm = k\bar{w}'$, and $\sum h' = M'$. Then from $hm = k\bar{w}$ and $h'm = k\bar{w}'$ follows that

$$k = \frac{hm}{\bar{w}} \qquad h'm = \frac{hm}{\bar{w}}\,\bar{w}'.$$

Then if $\Theta = \frac{\bar{w}}{\bar{w}'}$, $h = \frac{h'\bar{w}}{\bar{w}'} = h'\Theta$, and $h' = \frac{h}{\Theta}$.

Let r be the number of letters omitted in P, then

$$\bar{w} = \frac{n!}{g!\,h!\,k!-\,-\,a^g\,b^h\,c^k-\,-\,r!}$$

and

$$\bar{w}' = \frac{(n-\ell)!}{g!\,h!\,k!-\,-\,a^g\,b^h\,c^k-\,-\,(r-\ell)!}$$

where P is a substitution containing g cycles of a letters, h cycles of h letters, etc.

$$\text{Then } \frac{1}{\Theta} = \frac{\bar{w}'}{\bar{w}} = \frac{(n-\ell)!}{g!\,h!\,k!-\,-\,a^g\,b^h\,c^k-\,-\,(r-\ell)!} \times \frac{g!\,h!\,k!-\,-\,a^g\,b^h\,c^k-r!}{n!}$$

$$= \frac{r(r-1)(r-2)-\,-\,-(r-\ell+1)}{n(n-1)(n-2)-\,-\,-(n-\ell+1)}$$

$$mM' = (n')! \qquad M' = \frac{(n')!}{m} = \frac{(n')!}{n!} \quad M = \frac{(n-\ell)!}{n!} \qquad M = \frac{M}{n(n-1)-(n-\ell+1)}$$

Then $\sum \frac{h}{\theta} = M'$ for $h' = \frac{h}{\theta}$. If we substitute in this sum, the values of $\frac{h}{\theta}$ and M' just derived we have

$$\sum \frac{hr(r-1)---(r-\ell+1)}{n(n-1)---(n-\ell+1)} = \frac{M}{n(n-1)(n-2)--(n-\ell+1)}$$

Since the sum here effects only the h and r, this reduces to

$$\sum hr(r-1)---(r-\ell+1) = M \quad (1).$$

Let 1, P, Q --- be the substitution of the group, and H_{n-r} the number of these substitutions involving n - r letters. The values of h, corresponding to all the substitutions on n - r letters, irrespective of the form, are multiplied by the same quantity in the above summation (1) so that for (1) we may now write

$$\sum r(r-1)---(r-\ell+1)H_{n-r} = M.$$

where the summation applies to the various values of r.

This formula will hold then when the group is simply transitive, doubly transitive -- till it is l-fold transitive. That is, ℓ may be taken equal to 0, 1, 2, 3 --- $\ell - 1$. If $\ell = 0$

$$\sum H_{n-r} = M.$$

(1) $M = H_n + H_{n-1} + H_{n-2} + - - - H_2 + 1$. $H_0 = 1$ for this is simply the identity. $H_1 = 0$ for this is the substitution that replaces a single letter.

If $\ell = 1$. $\sum H_{n-r} = M$.

(2) $M = H_{n-1} + 2H_{n-2} + - - - (n-2)H_2 + n$.

$\ell = 3$ $\sum r(r-1)(H_{n-r}) = M$.

(3) $M = 2.1\, H_{n-2} + 3{:}H_{n-3} + - - (n-2)(n-3)H_2 + (n-1)n$.

$$\ell = \ell. \quad \sum r(r-1)---(r-\ell+1)H_{n-r} = M.$$

(4) $M = - - - \ell!\, H_{n-\ell} + - - - (n-\ell+1) -- (n-1)n$.

It is from these formulas that the theorem as to the aver-

age number of letters in the substitutions of a transitive group arises. From (1) no conclusion can be drawn as to transitive groups for a group that is intransitive on n - ℓ letters, if $\ell = 0$, is an intransitive group. From (2) however the theorem is evident. There is no substitution involving n letters; the H_{n-2} is multiplied by 2, H_{n-3} by 3, H_{n-4} by 4, so the average number of letters is brought up to n - 1. The same conclusion can be drawn from the other equations. Although Cauchy was here very close to this important theorem, he did not enunciate it.

If $\mathcal{E}_n$ designates the sum of the first n + 1 terms of the expansion of $\mathcal{E}^{-1}$, and $[n]_r$ the first r + 1 terms of the development of $(1 - 1)^n$, then we have the following table, formed by multiplying the equations (1), (2), (3), (4) - - above by 1, -1, $\frac{1}{2}$ - - - $\frac{(-1)^{\ell}}{\ell!}$ M, respectively, and taking the sum. The reason for this process is found in the theorem stated but not proved by Cauchy that

$$\sum \frac{1}{g!\,h!\,k! - - a^g \; b^h \; c^k} = \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - - \frac{(1)^n}{n!}$$

where the g, h, k - - a, b, c, indicate a substitution of g cycles of order a, h cycles of order b, k cycles of order c - - - and the sum includes only such cycles as involve more than one letter.

$$M = H_n + H_{n-1} + H_{n-2} + H_{n-3} + H_{n-4} - - - - + H_2 + 1$$

$$-M = - H_{n-1} - 2H_{n-2} - 3H_{n-3} - 4H_{n-4} - - - -(n-2)H_2 - n$$

$$\frac{M}{2} = \frac{2}{2!} H_{n-2} + \frac{3 \cdot 2}{2!} H_{n-3} + \frac{3 \cdot 4}{2!} H_{n-4} \quad \frac{+(n-3)(n-2)}{2!} H_2 + \frac{n(n-1)}{2!}$$

$$-\frac{M}{3} = \frac{3 \cdot 2 \cdot 1}{3!} H_{n-3} - \frac{4 \cdot 3 \cdot 2}{3!} H_{n-4} \quad \frac{-(n-4)(n-3)(n-2)}{3!} H_2 - \frac{(n-2)(n-1)n}{3!}$$

$$\frac{(-1)^{\ell}}{\ell!} M = (-1)^{\ell} \frac{\ell!}{\ell!} H_{n-\ell} \;--\; + \left[(-1)^{\ell} (n - \ell + 1) - - - (n-1)n \right]$$

$$m(1 - 1 + \tfrac{1}{2} - \frac{1}{2.3} - -) = M_{\varepsilon} =$$

$$H_n + (1-1)H_{n-1} + (1-2+\tfrac{2!}{2})H_{n-2} + (1-3+\frac{3.2}{1.2} - \frac{3.2.1}{1.2.3})H_{n-3} + (1-4+\frac{4.3}{1.2} -$$
$$\frac{4.3.2.1}{1.2.3.4})H_{n-4} + - - - \quad (1-\ell+\frac{\ell(\ell-1)}{2!} - \frac{\ell(\ell-1)(\ell-2)}{3!} + - - +(-1)^{\ell}$$
$$\frac{\ell(\ell-1)(\ell-2) - - -2\cdot 1}{\ell!} H_{n-\ell} + \Big[1-(1+\ell) + \frac{(\ell+1)\ell}{2!} - \frac{(\ell+1)(\ell)(\ell-1)}{3!} +$$
$$\frac{(\ell+1)(\ell)(\ell-1)(\ell-2)}{4!} - - - +(-1)^{\ell}\frac{(\ell+1)(\ell)(\ell-1) - - - 2\cdot 1}{\ell!} H_{n-(\ell+1)}$$
$$+ 1-(\ell+2) + \frac{(\ell+2)(\ell+1)}{2!} - \frac{(\ell+2)(\ell+1)\ell}{3!} + \frac{(\ell+2)(\ell+1)(\ell-1)(\ell)}{4!} - - -$$
$$\frac{(-1)^{\ell}(\ell+2)(\ell+1)(\ell)(\ell-1) - - 2\cdot 1}{\ell!} - - - - + \Big[1-(n-2)+\frac{(n-2)(n-3)}{2!}$$
$$- - - - + \frac{(-1)^{\ell}(n-2)(n-3) - - (n-\ell+1)}{\ell!}\Big] H_2 + \Big[1-n+\frac{n(n-1)}{2} - - -$$
$$- - \frac{(-1)^{\ell}(n)(n-1) - - (n-\ell+1)}{\ell!}\Big]$$

All the terms from the first to the term involving $H_{n-\ell-1}$ vanish because of the ℓ-fold transitivity of the group and the formula for the sum then reduces to

$M = H_n + [\ell+1]_{\ell} H_{n-\ell-1} + [\ell+2]_{\ell} H_{n-\ell-2} - - - [n-2]_{\ell} H_2 + [n]_{\ell}$ where $[n]$ has the significance indicated above.

If instead of taking the sum of all the equations in the series above (1) (2) (3) - - (4) the first had been suppressed and the sum of the remaining ℓ-s after multiplying each by a term in the expansion of ε^{-1}, a formula would arise that would involve (5) and be more general.

$$M = r!\,H_{n-r} + (r+1)(r) - - - 2H_{n-r-1} + (r+2)(r+1) - - 3H_{n-r-2} + - - -$$
$$+ (\ell+1)(\ell) -- (\ell-r+2)H_{n-\ell-1} + (\ell+2)(\ell+1)(\ell) - - - (\ell-r+3)H_{n-\ell-2}$$
$$+ - - - - (n-2) - - - (n-r-1)H_2 + n(n-1)(n-r+1).$$

$$-M = -(r+1)(r) - - - 1\,H_{n-r-1} - (r+2)(r+1) - - .2\,H_{n-r-2} - - -$$
$$(-)(\ell+1)(\ell) -- (\ell-r+1)H_{n-\ell-1} - (\ell+2)(\ell+1)(\ell) - - - (\ell-r+2)H_{n-\ell-2}$$
$$- - - - (n-2) - - - (n-r-2)H_2 - n(n-1)(n-r).$$

$$\frac{M}{2} = +\frac{1}{2!}(r+2)(r+1) - - - 1\,H_{n-r-2} + - - - \frac{1}{2}$$
$$(\ell+1)(\ell) - - (\ell-r)H_{n-\ell-1} + \frac{(\ell+2)(\ell+1)(\ell) - - (\ell-r+1)}{2!} H_{n-\ell-2}$$
$$+ - - - \frac{1}{2!}(n-2) - - (n-r-3)H_2 + n(n-1) - - - (n-r-1).$$

$$(-1)^{\ell}\frac{M}{\ell!} = \frac{(-1)^{\ell}}{\ell!}(\ell+1)(\ell) - - - 2H_{n- -1}$$
$$+ \frac{(-1)^{\ell}}{\ell!}(\ell+2)(\ell+1)(\ell) - - - - 3\,H_{n-\ell-2} + - - - (-1)^{\ell}$$
$$\frac{(n-2) --- (n-\ell-1)}{\ell!} + (-1)^{\ell}\frac{n(n-1) --- (n-\ell+1)}{\ell!}$$

$$Me_{\ell-r} = r!\,H_{n-r} + \Big[(\ell+1)(\ell) --- (\ell-r+2)\Big]\Big[1 - (\ell-r+1) + \frac{(\ell-r+1)(\ell-r)}{2!}$$
$$- \frac{(\ell-r+1)(\ell-r)(\ell-r-1)}{3!} ------- \frac{(\ell-r+1) ---- 2}{(\ell-r)!}(-1)^{(\ell-r)}\Big]$$
$$H_{n-\ell-1} + \Big[(\ell+2) --- (\ell-r+3)\Big]\Big[1 - (\ell-r+2) + \frac{(\ell-r+2)(\ell-r+1)}{2!}$$
$$- - - - + \frac{(\ell-r+2) --- 3}{(\ell-r)!}(-1)^{(\ell-r)}\Big]H_{n-\ell-2} + - - - - - -$$
$$\Big[(n-2) - - - (n-r-1)\Big]\Big[1 - (n-r-2) + \frac{(n-r-2)(n-r-3)}{2!} - - - -$$
$$\frac{(n-r-2) --- (n-\ell-1)}{(\ell-r)!}\Big]H_2 + \Big[n(n-1) ---- (n-r+1)\Big]\Big[1 -- (n-r) +$$
$$\frac{(n-r)(n-r-1)}{2!} - \frac{(n-r)(n-r-1)(n-r-2)}{3!} --- \frac{(n-r)(n-r-1) -- (n-\ell+1)}{(n-r)!}$$

Expressing this formula in the simpler form by means of $[n]_r$ already defined we have

$$M\varepsilon_{\ell-r} = r!\,H_{n-r} + (\ell+1) --- (\ell-r+2)\big[\ell-r+1\big]_{\ell-r} H_{n-\ell-1} + (\ell+2) - - -$$

$$(\ell-r+3)\big]\big[\ell-r+2\big]_{\ell-r}\, H_{n-\ell-2} + \cdots \frac{(n-2) \cdots (n-r-1)}{}\big[n-r-2\big]_{\ell-r}$$

$$H_2 + n(n-1) \cdots (n-r+1)\big[n-r\big]_{\ell-r} .$$

Transposing and dividing by factorial r we have

$$(6)\ H_{n-r} = \frac{M}{r!}\mathcal{E}_{\ell-r} - \frac{(\ell+1) \cdots (\ell-r+2)}{r!}\big[\ell-r+1\big]_{\ell-r}\, H_{n-\ell-1} -$$

$$\frac{(\ell+2) \cdots (\ell-r+3)}{r!}\big[\ell-r+2\big]_{\ell-r}\, H_{n-\ell-2} - \cdots - (n-2)(n-1)$$

$$\frac{(n-2)(n-1) \cdots (n-r-1)}{r!}\big[n-r-2\big]_{\ell-r}\, H_2\ \frac{-n(n-1) \cdots (n-r+1)}{r!}$$

$$\big[n-r\big]_{\ell-r} .$$

All the terms following the first are integral for a succession of r integers is always divisible by r !. The first term is also integral as Cauchy shows by simple means.

Let r, the number of letters omitted in a given substitution be equal to ℓ, then the formula for H_{n-r} becomes

$$H_{n-\ell} = \frac{M}{\ell!} - \frac{(\ell+1) \cdots 2}{\ell!}\, 2H_{n-\ell-1} - \frac{(\ell+2) \cdots 3}{\ell!}\, H_{n-\ell-2} - \cdots$$

$$\frac{(n-2) \cdots (n-\ell-1)}{\ell!}\, H_2 - \frac{n(n-1) \cdots (n-\ell+1)}{\ell!} .$$

Then if the number of letters omitted is $r = \ell-1$, H_{n-r} becomes

$$(1)\ H_{n-\ell+1} = \frac{(\ell+1) \cdots 4.3}{(\ell-1)!}\, H_{n-\ell-1} + \frac{(\ell+2) \cdots 4}{(\ell-1)!}\, 2\, H_{n-\ell-2} - \cdots$$

$$+ \frac{(n-2) \cdots (n-\ell)}{\ell!}\,(n-\ell-2)\, H_2 + \frac{n(n-1) \cdots (n-\ell+2)}{(\ell-1)!}(n-\ell)$$

Then if the group is simply transitive and $\ell = 1$

$$(2)\ H_n = H_{n-2} + H_{n-3} \cdots + (n-3)\, H_2 + (n-1).$$

From (1) we see that since all the terms are positive, it must follow that

$$H_{n-\ell+1} \overset{=}{>} \frac{n(n-1)(n-2) -- (n-\ell+2)}{(\ell-1)!} (n-\ell.$$

From (2) follows, when the group is simply transitive

$$H_n \overset{=}{>} n-1.$$

These results are included in the theorems:

(1) If G is an ℓ-fold transitive group of degree n, the number of substitutions involving $n-\ell+1$ letters is equal to or greater than $\frac{n(n-1) -- (n-\ell+2)}{\ell!} (n-\ell.$

(2) If G is a simply transitive group of degree n, the number of substitutions involving n letters is equal or greater than n-1.

Thus far, with the exception of one or two incorrect signs, the formulas and theorems are correct but a serious error follows immediately. We find the assertion that if in an ℓ-fold transitive group, $\ell + 1$ letters are left fixed, all are fixed. That this is false may be demonstrated by considering the imprimitive group of order 72 and degree six. It is simply transitive and so $\ell = 1$, but $\ell + 1 = 2$ letters may be left fixed without all becoming so.

Upon the basis of this assertion Cauchy says that formula (6) reduces to

$$H_{n-r} = \frac{M}{r!} E_{\ell-r} - \frac{n(n-1) --- (n-r+1)}{r!} [n-r]_{\ell-r} .$$

He then, by putting in definite values for ℓ, 0, 1, 2 - - - - - $\ell-1$, ℓ, derives the formulas,

$$H_n = ME_{\ell} - [n]_{\ell}$$

$$H_{n-1} = ME_{\ell-1} - \frac{n}{1} [n-1]_{\ell-1}$$

$$H_{n-2} = \frac{M}{2!} E_{\ell-2} - \frac{n(n-1)}{2!} [n-2]_{\ell-2}$$

$$H_{n-l+1} = \frac{M}{(l-1)!} E_1 - \frac{n(n-1) --- (n-l+2)}{(l-1)!} [n-l+1]_1$$

$$H_{n-l} = \frac{M}{l!} E_0 - \frac{n(n-1) --- (n-l+1)}{l!} [n-l]_0$$

Let us apply these formulas to this same imprimitive group of degree 6 and order 72.

$$H_6 = ME_l - [n]_l = -(1-\frac{n}{1}) = n-1. \qquad l = 1$$

There are 40 substitutions in this group involving all the letters.

$$H_5 = ME_0 - n[n-1]_0 = 72 - 6 = 66.$$

There are 12 substitutions in this group of degree 5.

Cauchy then applies this theorem to the special case of the symmetric group. Here $l = n-1$ and the following formulas arise.

$$H_n = n! E_n$$

$$H_{n-1} = n! E_{n-1}$$

$$H_{n-2} = \frac{n!}{2!} E_{n-2}$$

$$H_3 = \frac{n!}{(n-3)!} E_3$$

$$H_2 = \frac{n!}{(n-2)!} E_2$$

Suppose that n = 5.

$$H_n = 5! E_5 = 5! \frac{11}{30} = 44$$

$$H_{n-1} = 5! E_4 = 5! \frac{3}{8} = 45.$$

$$H_{n-3} = \frac{5!}{2!} E_3 = \frac{5!}{2!} \frac{1}{3} = \frac{40}{2!} = 20.$$

$$H_{n-4} = H_2 = \frac{5!}{3!} \frac{1}{2} = 10.$$

Hence the formula applies to the symmetric group.

The alternating group is n-1 times transitive; then $l = n-2$

and

$$H_n = \frac{n!}{2} E_{n-2} - (-1)^n (n-1)$$
$$H_{n-1} = \frac{n!}{2} E_{n-3} - (-1)^{n-1} n(n-2)$$
$$H_{n-2} = \frac{n!}{2} \frac{E_{n-4}}{2!} - (-1)^{n-2} \frac{n(n-1)}{2!} (n-3)$$
$$HH_3 = \frac{n!}{2} \frac{E1}{(n-3)!} - (-1)^3 \frac{n(n-1) \cdots 4}{(n-3)!} 2$$
$$H_2 = \frac{n!}{2} \frac{E0}{(n-2)!} - (-1)^2 \frac{n(n-1) \cdots 3}{(n-2)!}$$

The last two reduce to

$$H_3 = \frac{n(n-1)(n-2)}{3}$$
$$H_2 = 0.$$

This shows that the alternating group contains $\frac{n(n-1)(n-2)}{3}$ cyclic substitutions of order 3 and no transposition.

So while these latter formulas hold for the special cases of the alternating and symmetric groups they do not hold in general. However, the assumption upon which these formulas are based are true of the alternating and symmetric groups; that is, the symmetric group is intransitive when the number of letters left fixed is n-1; so since here $l = n-1$, then $l+1 = n$ and all the letters are left fixed as the assumption requires. If the alternating group be considered, $l = n-2$; $l+1 = n-1$ and if n-1 letters of the alternating group are left fixed, certainly all are.

Another theorem stated correctly by Cauchy but containing errors in the proof is the following.

Given two groups of degree n

$$1, P, Q, R, ---$$

and $1, P', Q', R', ---$, one of order M, the other of order M'. Then if E is the number of substitutions that

transform one group into the other, n and E are congruent, mod, MM'.

The proof is as follows:

Suppose the group 1, P, Q, R - - - is the group belonging to a function Ω. Let U be such that $U^{-1}PU = P'$ and $U^{-1}\Omega U' = \Omega'$.

Then $(PU)^{-1}\Omega PU = \Omega'$ and

$(UP')^{-1}\Omega UP' = \Omega'$.

Hence $P'^{-1}U^{-1}\Omega UP' = \Omega'$.

$U'\Omega U = \Omega'$ so $P'^{-1}\Omega' P' = \Omega'$.

<u>Then the substitutions that do not change</u> Ω are

U, UP, UQ, UR, - - -

This statement is evidently false for by hypothesis U transforms Ω into Ω'. If it transformed Ω' into itself, its inverse would also, but the inverse would have to transform Ω' into Ω and so Ω and Ω' would be identical.

The remainder of the proof is correct. U and UP' transform Ω into Ω' so U^{-1} and $(UP')^{-1} = P'^{-1}U^{-1}$ transform Ω' into Ω. Then $UP'U^{-1}$ transforms Ω into itself and so evidently belongs to the group 1, P, Q, R - - -.

Then the number E, of substitutions that satisfy the equation,

$PU = UP'$ is the product of M by the number of functions $\Omega, \Omega', \Omega''$, - - - not changed by one or more substitutions of the group 1 P' Q' R' - - - and the theorem follows.

The theorem that the holomorph of a cyclic group is the product of the cyclic group and its group of isomorphisms is found implicitly in Cauchy. The theorems he gives may be stated as follows:

1. Let $P = (x_0\ x_1\ x_2\ - - -\ x_n)$ be a substitution of

order n. Let r be a primitive root of the modulus n and I the smallest of the indices of unity corresponding to the base r. Then let Q be a substitution that replaces x by x_r . The order of Q will be I and the order of the group generated by P and Q will be n .

This I is nothing else than the order of the group of isomorphisms of the cyclic group and so this group of order n_I is the holomorph of the cyclic group. If n is a power of a prime then I = $n(1 - \frac{1}{p})$ where p is the prime. When n is a prime I = n-1.

2. With the same hypothesis as in (1) P^a and Q^b, where a and b are divisors of n and I respectively, generate a group of order $\frac{n\,I}{a\,b}$.

Cauchy was the first to attempt an enumeration of the possible orders of groups. This he did with a fair degree of accuracy up to and including the sixth degree. The enumerations including degree five are correct and complete but several errors occur in his enumerations of the possible orders of groups of degree six. For instance (2) 150 is given as the index of a group of degree six under the symmetric group when 6 ! is not a multiple of 150.

Cauchy goes back to his original distinction between imprimitive groups with heads direct products and those with heads formed by isomorphisms. He gives (3) as the possible orders of groups of degree 6 with heads direct products of the transitive constituents 72, 48, 24, 18, 16, 8. The last two numbers are clearly impossible for there is no transitive group even of degree 6 and order 8 or 16.

(1) Oeuvres, Vol. 9, p. 333
(2) " , " ", p. 494
(3) " , " ", p. 495

The orders of the groups possible when the head is formed by isomorphisms are given as 6, 12, 4 while there is no imprimitive group of order 4 and degree 6. According to his classification too there should also be included in this last enumeration 24 and 18. A complete omission occurs in imprimitive groups since the groups of order 36 with two systems of imprimitivity are entirely omitted. Otherwise the enumeration through degree six is correct and complete.

In conclusion then we may say that the foundation period in the history of group theory includes the time from Lagrange through Cauchy; that at the beginning of the period group theory was a means to an end and not as end in itself. Lagrange and Ruffini thought of substitution groups only in so far as they lead to practical results in the theory of equations. Galois, while broadening and deepening the application to the theory of equations, still showed a slight break, developing his theory of substitutions, then applying it. In this respect he may be considered as taking an initial step toward abstract group theory. In Cauchy a group is still spoken of as the substitutions that leave a given function invariant; the order of a group is still the number of equal values the function assumes when the variables are permuted in every possible manner; but quite as often the group is "a system of conjugate substitutions" and its relation to a function is entirely ignored. It is due largely to this fact that Cauchy may be considered the founder.

Errors in Cauchy's Work on Group Theory.

The errors in Cauchy's work relating to group theory may be divided into two classes of varying importance; first, those which arise in the subject matter itself, and false statements about matters of fundamental importance; second, a large number of minor mistakes where the thought is evidently correct and the error arises only through careless statements. The errors of the first class have been included in the discussion of the theorems to which they apply. Among the minor errors we note the following:

I. Journal de l' Ecole polytechnique, 1845, p.19, 3rd par., line 24, "at least thirteen values" should read "at least eleven values".

II. Exercises, Vol. 3.

(1) Page 205, line 15.

$P = (x, y, z)(u, v, w)$ is called a substitution of order two.

(2) Page 218, (27) and (28).

From $\theta = \frac{a}{k} = \frac{b}{h} = \frac{n}{hk} = \frac{ab}{n}$ is derived the relation

$= \left(\frac{ab}{hk}\right)^{\frac{1}{2}}$ which should be $\theta = \frac{ab}{hk}$.

(3) Page 240 (22).

$Q = x_1\ x_2\ x_4\ x_8\ x_5 \cdot x_3\ x_6$ is called a substitution of order 6. From the derivation of Q it is evident that it should be of order six and its form

$$Q = x_1\ x_2\ x_4\ x_8\ x_7\ x_5 \cdot x_3\ x_6 .$$

(4) Page 241, 3rd line.

$3 \cdot 9$ is given as the order of a subgroup of the holo-

morph of degree nine, when $3 \cdot 6 = 18$ should be the order given.

(5) Page 178, Problem 2 should read, "Being given two substitutions P and R - - - ".

As a whole the Exercises are free from error. It is in the memoirs published in the Paris Comptes rendus that they are frequently found.

Oeuvres de Cauchy, Vol. 9.

(1) Page 303. The last line of the first paragraph reads, "$n' = n$ if the sets formed in this way reduce to two, the first of n-1 letters, the second of n only". Clearly n letters can not be divided into sets of n-1 and n letters and the n of the second set should be one.

(2) Page 315,.,Theorem II. "Let $\alpha/\beta\gamma$ - - -, $\lambda\mu.\nu$ - - - be two sets of n letters", should be "let $\alpha\beta\gamma$ - - -, $\lambda\mu\nu$ - - - be two sets of a letters".

(3) Page 322, line 1, reads "If the number a reduces to unity, it signifies that, the variable n becoming fixed, all the others become fixed also". Evidently n should be x, for n is not a variable.

(4) Page 327, (13).

P, PQ, P^2Q - - - $P^{a-1}Q$ should be Q, PQ, P^2Q - - - $P^{a-1}Q$.

(5) Page 376, 1st line.

$M - K$ should read $m - K$.

(6) Page 382, Theorem VI. The hypothesis should read: Let Ω be a function of several independent variables; let Ω Ω' - - be the distinct values of this function

and m their number - - -, instead of m the number of equal values of the function.

(7) Page 390, Formula (11). The fourth line should read $\frac{(n-2)\,-\,-\,-\,(n-r-1)}{r!}\left[n-r-2\right]_{\ell-r} H_2$. Cauchy uses the correct form and not the form as printed, to develop his later formulas.

(8) Page 392, Formula (14). For $\frac{(n-1)(n-2)\,--\,(n-\ell)}{(\ell-1)!}\left[n-\ell-2\right] H_2$ in the second line, we should have

$$\frac{(n-2)\,-\,-\,-\,(n-\ell)}{(\ell-1)!}\,(n-\ell-2)\,H_2\ .$$

(9) Page 397, last line. $U^{-1} = PU^{-1}$ should be $U^{-1} = PU'^{-1}$.

(10) Page 399, line 16. Table (5) should be Table (9)

(11) Page 404, line 18. The inverse of $P'U$ is given as $U'P'^{-1}$ and should be $U^{-1}P'^{-1}$.

(12) Page 406. In the memoir on Bertrand's memoir, there is the statement that a function on six letters can not assume more than six values, when it should be that it can not assume less.

(13) Page 422. The last two lines should be

$(x\ y\ z)\,(u)\,(v) \quad (y\ z\ x)\,(u)\,(v) \quad (z\ x\ y)\,(u)\,(v)$

$(x\ y\ z)\,(v)\,(u) \quad (y\ z\ x)\,(v)\,(u) \quad (z\ x\ y)\,(v)\,(u)$

(14) Page 429, Problem II This should read: Given two substitutions P and R find Q.

(15) Page 434, (9). $P = (\alpha\,\alpha'\,\alpha''\,-\,-\,-\,\beta\,\beta'\,\beta''\,-\,-\,\varphi\,\varphi'\,\varphi'')$

should be $P = (\alpha\,\alpha'\,\alpha''\,-\,-\,-\,\lambda\,\lambda'\,\lambda''\,-\,-\,\varphi\,\varphi'\,\varphi'')$

(16) Page 448. The last line of corollary II should read, two irregular substitutions of the sixth order instead of the fourth.

(17) Page 474. In the table

$$P_0 = P_{n-1} = P_{2(n-1)} - - - = P$$

the second line should be

$$P_1 = P_n = P_{2n-1} - - - = P' P P'^{-1}$$

instead of $P_\ell = - - -$.

(18) Page 491, line 14. We can form a transitive function of three letters that offers only three or six distinct values, should read we can form a transitive function of <u>four</u> letters instead.

(19) Page 504, line 14, for "twenty distinct values and six equal values", there should be twenty equal values and six distinct.

Errors in Vol. 10 Oeuvres.

Page 8, line 5.

$\bar{W}_1$ should be $\bar{W}_4$.

Page 10, line 14.

Formula (14) should be formula (16). The same correction should be made in line 20.

Page 12, (22). $P' P = P'' P$ should be $P P' = P'' P$.

Page 20, line 12. For three distinct values there should be twelve distinct values.

Page 23, line 12.

$T = Q S Q^{-1} S Q \qquad T = S Q^{-1} Q S Q^{-1}$ should be

$T = Q S Q^{-1} S Q \qquad T = Q^{-1} S Q S Q^{-1}$.

Page 32, line 20. Put U for v.